

TC2100

RANDOLPH

Organization

Bldg./Room

U. S. DEPARTMENT OF COMMERCE

COMMISSIONER FOR PATENTS

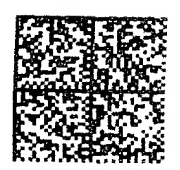
P.O. BOX 1450

ALEXANDRIA, VA 22313-1450

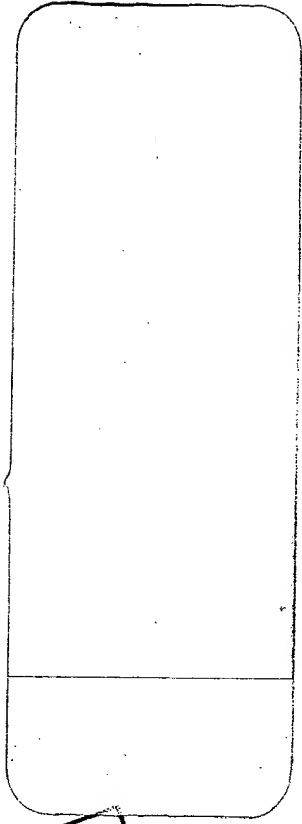
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPLOYER



UNITED STATES POSTAGE
U.S. OFFICIAL MAIL
PENALTY FOR
PRIVATE USE \$300
02 1A
0004205065
MAILED FROM ZIP CODE 22314
SEP 26 2005
\$ 02.219
PATNEY HOWES



U.S. POST MAIL CENTER
SEP 26 2005
RECEIVED

BEST AVAILABLE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

7590 09/26/2005
NIXON PEABODY LLP
8180 GREENBORO DRIVE
SUITE 800
MCLEAN, VA 22102

RECEIVED
OICE/IAP

SEP 27 2005

EXAMINER

DARROW, JUSTIN T

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 09/26/2005

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/534,756	03/24/2000	Thanh T. Ta	D/A0004	2748

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTION OF DIGITAL WORKS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1400	\$0	\$1400	12/27/2005

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. **PROSECUTION ON THE MERITS IS CLOSED.** THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN **THREE MONTHS** FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. **THIS STATUTORY PERIOD CANNOT BE EXTENDED.** SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE REFLECTS A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE APPLIED IN THIS APPLICATION. THE PTOL-85B (OR AN EQUIVALENT) MUST BE RETURNED WITHIN THIS PERIOD EVEN IF NO FEE IS DUE OR THE APPLICATION WILL BE REGARDED AS ABANDONED.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail**

**Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571) 273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

7590 09/26/2005

**NIXON PEABODY LLP
8180 GREENBORO DRIVE
SUITE 800
MCLEAN, VA 22102**

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/534,756	03/24/2000	Thanh T. Ta	D/A0004	2748

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTION OF DIGITAL WORKS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1400	\$0	\$1400	12/27/2005

EXAMINER	ART UNIT	CLASS-SUBCLASS
DARROW, JUSTIN T	2132	380-240000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
 (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
 (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
 1 _____
 2 _____
 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are enclosed:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):

- ☐ A check in the amount of the fee(s) is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above. NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/534,756	03/24/2000	Thanh T. Ta	D/A0004	2748

7590 09/26/2005
NIXON PEABODY LLP
8180 GREENBORO DRIVE
SUITE 800
MCLEAN, VA 22102

EXAMINER

DARROW, JUSTIN T

ART UNIT PAPER NUMBER

2132

DATE MAILED: 09/26/2005

Determination of Patent Term Extension under 35 U.S.C. 154 (b) (application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571) 272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

Notice of Allowability

Application No.

09/534,756

Examiner

Justin T. Darrow

Applicant(s)

TA ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendments filed 10/22/2004 and 11/16/2004.
2. ☒ The allowed claim(s) is/are 1-4,6-14,19,20,22-26,30 and 31.
3. ☒ The drawings filed on 22 October 2004 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Art Unit: 2132

DETAILED ACTION

1. Claims 1-34 have been presented for examination. Claims 1, 11-24, and 30 have been amended in an amendment filed 10/22/2004. Claims 1-4, 6, 9, 13, and 24 have been amended and claims 5, 15-18, 21, 27-29, and 32-34 have been cancelled in an amendment filed 11/16/2004. Claims 1-4, 6-14, 19, 20, 22-26, 30, and 31 have been examined.

Priority

2. Acknowledgment is made that the instant application is a continuation-in-part of Application No. 09/178,529, filed 10/23/1998, now U.S. Patent No. 6,519,700 B1.

3. Under 35 U.S.C. 120, a claim in a U.S. application is entitled to the benefit of the filing date of an earlier filed U.S. application if the subject matter of the claim is disclosed in the manner provided by 35 U.S.C. 112, first paragraph, in the earlier filed application. See MPEP § 201.11 I. and *Tronzo v. Biomet*, 156 F.3d 1154, 47 USPQ2d 1829 (Fed. Cir. 1998).

Priority is not granted for claims 1-4, 6-14, 19, 20, 22-26, 30, and 31 with respect to Application No. 09/178,529, filed 10/23/1998, because the subject matter of the claims is not disclosed in the manner provided by 35 U.S.C. 112, first paragraph, in the earlier filed application.

As per claims 1-4 and 6-12, Application No. 09/178,529 neither describes nor enables the limitation:

polarizing the system resource in accordance with a second polarization scheme using the polarization seed (see page 10, lines 10-17; figure 4, items 410, 412, 418, and 420; the “polarization” step adapted to secure the document includes receiving a polarization key as a

Art Unit: 2132

polarization seed from the user's system and transforming the document in a single polarization scheme to a version having polarized contents, comprising; see page 5, lines 1-6; a document with a set of permissions and an executable code segment that includes most of the software necessary to extract and use the encrypted document contents, as the system resource).

In Application No. 09/178,529, the polarization of the digital work and the system resource is described and enabled as facilitated in a single step in the same polarization scheme with the polarization seed.

As per claims 13, 14, 19, 20, 22, and 23, Application No. 09/178,529 neither describes nor enables the limitation:

a system resource comprising a copy of a portion of the digital work's resource information, wherein the system resource has been polarized in accordance with a second polarization scheme using the polarization seed (see page 10, lines 10-17; figure 4, items 410, 412, 418, and 420; the "polarization" step adapted to secure the document includes receiving a polarization key as a polarization seed from the user's system and transforming the document in a single polarization scheme to a version having polarized contents, comprising; see page 5, lines 1-6; a document with a set of permissions and an executable code segment, as the digital work's resource information, that includes most of the software necessary to extract and use the encrypted document contents, as the system resource).

In Application No. 09/178,529, the polarization of the digital work and the system resource is described and enabled as facilitated in a single step in the same polarization scheme with the polarization seed.

Art Unit: 2132

As per claims 24-26, 30, and 31, Application No. 09/178,529 neither describes nor enables the limitation:

providing a polarized system resource, wherein the system resource has been polarized in accordance with a second polarization scheme using the polarization seed (see page 10, lines 10-17; figure 4, items 410, 412, 418, and 420; the “polarization” step adapted to secure the document includes receiving a polarization key as a polarization seed from the user’s system and transforming the document in a single polarization scheme to a version having polarized contents, comprising; see page 5, lines 1-6; a document with a set of permissions and an executable code segment that includes most of the software necessary to extract and use the encrypted document contents, as the system resource).

In Application No. 09/178,529, the polarization of the digital work and the system resource is described and enabled as facilitated in a single step in the same polarization scheme with the polarization seed.

Drawings

4. The drawings were received on 10/22/2004. These drawings are approved by the examiner.

Allowable Subject Matter

5. Claims 1-4, 6-14, 19, 20, 22-26, 30, and 31 are allowed.
6. The following is an examiner’s statement of reasons for allowance:

Art Unit: 2132

Claims 1, 7, 8, and 10; 13, 14, 19, 20, 22, and 23; 24-26; and 30 and 31 are drawn to a method of creating a polarized digital work, a computer readable medium for storing a protected digital work, and two methods of protecting a digital work during replay, respectively. The closest prior art, Moskowitz, U.S. Patent No. 6,598,162 B1 in view of Abraham et al., U.S. Patent No. 5,148,481 A, discloses a similar methods and a similar medium. Although Abraham et al. describes encrypting data keys with a host master key entered by the security administrator on behalf of the user (see column 13, lines 31-39; a security administrator entering a host master key into the network security processor for a user, with node master keys encrypted by the host master key), neither Moskowitz nor Abraham et al. teach or suggest a polarization seed comprising an authorization code for a user received from a trusted source. This particular feature explicitly recited in independent claims 1, 13, 24, and 30 renders claims 1, 7, 8, and 10; 13, 14, 19, 20, 22, and 23; 24-26; and 30 and 31, respectively, allowable.

Claims 2-4, 6, 9, and 11 are drawn to a method of creating a polarized digital work. The closest prior art, Moskowitz, U.S. Patent No. 6,598,162 B1, discloses a similar method. Although Moskowitz discusses audio content and resource information (see column 8, lines 3-8; in AIFF and WAV formats) and image media (see column 8, lines 3-8; in TIFF, PICT, JPEG, and GIF formats), he neither shows nor implies a video stream and resource information comprising sample rate, sample type, and sample form. This distinct feature explicitly recited in independent claim 11 renders claims 2-4, 6, 9, and 11 allowable.

Claim 12 is drawn to a method of creating a polarized digital work. The closest prior art, Moskowitz, U.S. Patent No. 6,598,162 B1, discloses a similar method. Although Moskowitz discusses audio content and resource information (see column 8, lines 3-8; in AIFF and WAV

Art Unit: 2132

formats) and image media (see column 8, lines 3-8; in TIFF, PICT, JPEG, and GIF formats), he neither describes nor motivates a first audio/video stream and a second audio/video stream and where the first audio/video stream is polarized and further comprising mixing the polarized first audio/video stream with the second audio/video stream. This particular limitation incorporated in independent claim 12 renders it allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Canal+ Societe Anonyme (Maillard et al.), International Application Publication No. WO 99/18729 A1 discloses audiovisual data scrambled received by a smart card, descrambled, encrypted, and forwarded to a receiver for rendering in clear form
- Maillard et al., U.S. Patent No. 6,286,103 B1 is a counterpart United States patent to Canal+ Societe Anonyme (Maillard et al.), International Application Publication No. WO 99/18729 A1

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed **“OFFICIAL FAX”**. Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only **“OFFICIAL FAX”** but also **“AMENDMENT AFTER FINAL”**.

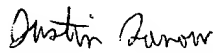
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

Art Unit: 2132

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

March 9, 2005


JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100

Interview Summary	Application No.	Applicant(s)	
	09/534,756	TA ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

All participants (applicant, applicant's representative, PTO personnel):

(1) Justin T. Darrow.

(3) Bijan Tadayon.

(2) Carlos R. Villama, Reg. No. 43,224.

(4) _____.

Date of Interview: 04 November 2004.

Type: a) ☐ Telephonic b) ☐ Video Conference
c) ☒ Personal [copy given to: 1) ☐ applicant 2) ☐ applicant's representative]

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☐ No.
If Yes, brief description: _____.

Claim(s) discussed: 1, 5, 11, 12, 29, and 34.

Identification of prior art discussed: Moskowitz, U.S. Patent No. 6,598,162 B1 and Canal+Societe Anonyme (Maillard et al.), International Application Publication No. WO 99/18729 A1.

Agreement with respect to the claims f) ☐ was reached. g) ☐ was not reached. h) ☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: See Continuation Sheet.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The amendment to claim 1 filed 10/22/2004 requires the digital content to remain polarized until it is input into the application. This step is not anticipated by Moskowitz, U.S. Patent No. 6,598,162 B1. However, Canal+Societe Anonyme (Maillard et al.), International Application Publication No. WO 99/18729 A1 describes an encrypted data stream introduced to a decoder coupled to a playing device. Although claims 5, 11, 12, 29, and 34 contain allowable subject matter over this reference, an update search on this subject matter will be conducted in the next Office action.

Notice of References Cited	Application/Control No. 09/534,756		Applicant(s)/Patent Under Reexamination TA ET AL.	
	Examiner Justin T. Darrow		Art Unit 2132	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,286,103 B1	09-2001	Maillard et al.	713/200
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	WO 99/18729 A1	04-1999	WIPO	MAILLARD et al.	H04N 07/16
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

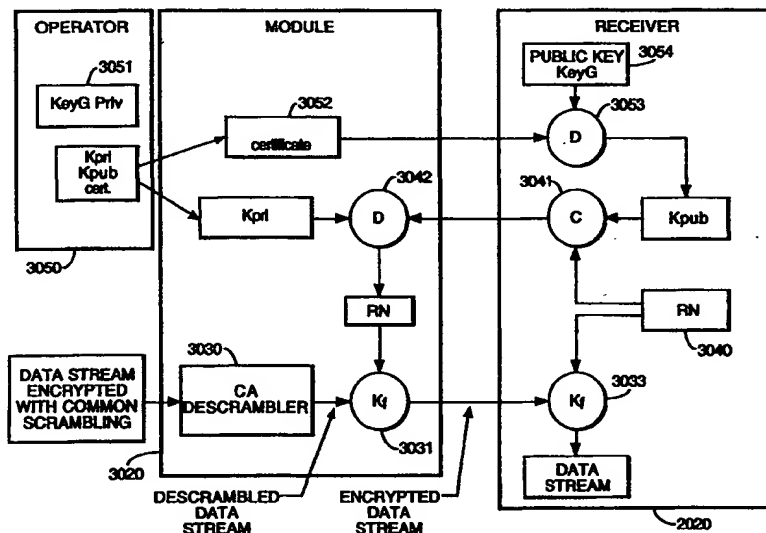
*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04N 7/16, 7/167		A1	(11) International Publication Number: WO 99/18729
			(43) International Publication Date: 15 April 1999 (15.04.99)
(21) International Application Number: PCT/IB98/01610		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 2 October 1998 (02.10.98)			
(30) Priority Data: 97402322.8 2 October 1997 (02.10.97) EP 98401388.8 9 June 1998 (09.06.98) EP 98401389.6 9 June 1998 (09.06.98) EP			
(71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André-Citroën, F-75711 Paris Cedex 15 (FR).			
(72) Inventors; and (75) Inventors/Applicants (for US only): MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal-Leclerc, F-28130 Maintenon (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F-77600 Bussy-Saint-Georges (FR). DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène-Manuel, F-75116 Paris (FR).			
(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).		Published With international search report.	

(54) Title: METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION



(57) Abstract

A method of transmission and reception of scrambled data in which the scrambled data is transmitted to a decoder (2020), the scrambled data being passed to and descrambled by a security module or smart card (3020) inserted in the decoder (2020) and characterised in that the scrambled data stream is passed from the smart card (2020) back to the decoder (3020) in an encrypted form. The encryption of the data stream may be carried out on the card (2020) or as a secondary encryption step at transmission. The data stream may correspond directly to audiovisual data descrambled in the security module or to a stream of control word data subsequently used by the decoder to descramble a transmission.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

-1-

METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM
TRANSMISSION

5 The present invention relates to a method and apparatus for use with an encrypted or scrambled transmission, for example a scrambled television broadcast.

10 Transmission of encrypted data is well-known in the field of pay TV systems, where scrambled audiovisual information is usually broadcast by satellite to a number of subscribers, each subscriber possessing a decoder or receiver/decoder capable of descrambling the transmitted program for subsequent viewing.

15 In a typical system, scrambled data is transmitted together with a control word for descrambling of the data, the control word itself being encrypted by a so-called exploitation key and transmitted in encrypted form. The scrambled data and encrypted control word are then received by a decoder having access to an equivalent of the exploitation key stored on a smart card inserted in the decoder to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive in a monthly ECM (Entitlement Control Message) the exploitation key necessary to decrypt the encrypted control word so as to permit viewing of the transmission.

25 In order to try to improve the security of the system, the control word is usually changed every ten seconds or so. This avoids the situation with a static or slowly changing control word where the control word may become publicly known. In such circumstances, it would be relatively simple for a fraudulent user to feed the known control word to the descrambling unit on his decoder to descramble the transmission.

30 Notwithstanding this security measure, a problem has arisen in recent years where the stream of control words sent during a broadcast film, for example, becomes known. This information may be used by any unauthorised user who has recorded the still-scrambled film on a video recorder. If the film is replayed at the same time as the stream of control words is fed to the decoder, visualisation of the film becomes

-2-

possible. Provided the user manages to synchronise the film with the control stream there are no great technical problems in carrying out such a fraud, particularly since the hardware elements necessary to build the descrambler are easily obtained.

- 5 This problem has been exacerbated with the rise of the internet and it is now not uncommon to find any number of internet sites that publish the stream of control words emitted during a given transmission.

- 10 It is an object of the present invention to overcome the problems associated with known prior art techniques for scrambled transmissions so as to provide a secure decoder configuration resistant to attacks such as those described above.

- 15 According to the present invention there is provided a method of transmission and reception of a scrambled data stream in which the scrambled data stream is transmitted to a decoder, and thereafter passed to and descrambled by a portable security module inserted in the decoder and characterised in that the data stream is passed from the security module to the decoder in an encrypted form, to be decrypted and subsequently used by the decoder.

- 20 As discussed above, in conventional systems, a control word is encrypted by an exploitation key and passed from the decoder to the smart card for decryption before being passed in a decrypted form to the control unit in the decoder for descrambling of the transmission. The weak point in such techniques lies in the transmission of the control word "in clear" between the card and the decoder unit, since it is relatively
25 easy to determine the connections between the card and the decoder and to thereafter record the control word information passing along these connections.

- 30 By identifying this weakness, and proposing a solution in which data is descrambled by a portable security module before being passed back to the decoder in an encrypted form the present invention overcomes the problems with these techniques.

According to a first type of realisation of the invention, the data stream is encrypted

-3-

in the security module by a first encryption key before being passed back to the decoder for decryption using an equivalent of the first key. However, as will be described below, other realisations of the invention are possible, in which the data is passed from security module to decoder in encrypted form but in which the encryption
5 takes place at the transmission level.

In one embodiment of the above realisation, the data stream is encrypted in the security module by a first encryption key variable in dependence on a decoder identity value, the decoder possessing an equivalent of the key and value necessary to decrypt
10 the data. For example, the decoder identity value can correspond to the serial or batch number of the decoder.

The decoder identity value may be encrypted by a personalised key known to the security module and transmitter, the decoder identity value being transmitted in an
15 encrypted form to the decoder for communication to the security module. Once decrypted by the personalised key within the security module the decoder identity value and first encryption key can be used by the security module to create the encrypted data stream.

20 Communication of the decoder identity value to the security module will necessarily involve a signal being sent from the decoder to the security module. As we have seen, the transmission of messages across this channel is relatively easy to monitor and it is thus preferable to transfer the identity value in a non-readable form to the security module.

25

Personalised keys of this type are known in relation to EMMs or Entitlement Management Messages, which transmit each month in encrypted form a management key for decrypting that month's ECM to a selected subscriber or group of subscribers possessing the necessary personalised key to decrypt the EMM.

30

In an another solution, the decoder identity value may be encrypted by a personalised key known to the security module, the encrypted decoder identity value being stored

-4-

in the decoder during manufacture of the decoder for communication to the security module upon insertion of the security module in the decoder.

5 In an alternative to the use of a fixed decoder identity value, the first encryption key may be dependent on a random or pseudo-random number generated, for example, by the decoder and communicated to the security module.

10 Preferably, and in view of the problems associated in communicating non-encrypted data between the decoder and the security module, the random number is encrypted by a second encryption key before being communicated between the decoder and security module, or vice versa.

15 In one embodiment, the random number may be generated and encrypted by a second encryption key at the decoder and communicated to the security module for decryption by an equivalent of this second key stored in the security module.

20 In an alternative embodiment, the operation of the security module and decoder may simply be reversed, such that the random number is generated and encrypted by a second key in the security module and communicated to the decoder for decryption by an equivalent of the second key stored in the decoder.

25 In the examples given above, the first and second encryption key, the personalised security module key etc may all be created in accordance with a known symmetric encryption algorithm, such as DES, RC2 etc. However, in a preferred embodiment where the decoder is responsible for generation of the random number, the second key used to encrypt the random number corresponds to a public key, the security module being provided with the equivalent private key necessary to decrypt the random number value.

30 As compared with a portable security module such as a smart card, the hardware component in the decoder used to store the first and second encryption keys (typically a ROM) is relatively easy to isolate and monitor by means of attached contacts etc.

A dedicated fraudulent user may therefore obtain the first and second keys and, by monitoring communications between the security module and decoder, the encrypted value of the random number. If a symmetric algorithm is used for the second key, the random number may then be decrypted with the known decoder second key and fed
5 to the known first key to decrypt the control word.

In contrast, through the use of a public key/private key arrangement, possession of the second public key held by the decoder does not enable a fraudulent user to decode the encrypted random number. Whilst it is always possible to obtain the random number
10 directly, this is more difficult in comparison with obtaining the keys and picking up the communicated encrypted value, since the random number will be most likely generated and stored somewhere in the RAM of the decoder and can in any case change on a regular basis.

15 Preferably, the second private key is unique to the security module. This embodiment substantially increases the security of the system, although as will be understood the data stream communicated between the security module and decoder will be in any case dependent on the random number generated during that session.

20 As mentioned above, the use of a public/private key arrangement in relation to the second encryption key is particularly advantageous where the private key is stored in the security module and the public key in the decoder. However, in alternative embodiments, the situation may be reversed such that the private key is held in the decoder and the public key in the security module.

25

Advantageously, the second decoder key is encrypted by a third key before communication to the decoder, the decoder possessing the corresponding third key so as to decrypt and verify the second decoder key.

30 In a particularly advantageous embodiment, the third key used to decrypt the second decoder key is a private key, the decoder possessing the equivalent public key to decrypt and verify the communicated second key.

-6-

In all of the above embodiments of this first type of realisation, the data stream is re-encrypted by a first encryption key held in the security module before being passed to the decoder.

5 As mentioned, in an alternative type of realisation, the encrypted data stream passed between the security module and decoder is prepared upstream of the security module. In such realisations, the data stream is encrypted at the point of transmission by a first encryption key and decrypted by the decoder by an equivalent of this key.

10 In a preferred embodiment, the data stream is encrypted at the point of transmission by a first encryption key dependant on a variable known to both the transmitter and the decoder and decrypted by the decoder by an equivalent of this key and variable.

For example, the data stream may be encrypted at the point of transmission by a first
15 encryption key dependant on the real time and/or date of transmission. In such a case, the encrypted data stream will only function at the time of transmission of the broadcast and cannot be fed into the descrambler of a decoder after the broadcast has been recorded since the decryption key of the decoder (or rather its associated variable) will now have changed.

20 As will be appreciated, whilst this realisation is less secure than the embodiments of first realisation discussed above, it possesses the advantage that no changes to the hardware of existing security modules are necessary. Furthermore, the modifications to the decoder and transmitter needed to implement the invention can be implemented
25 in software, e.g. in the case of the decoder by the downloading of transmitted data.

In this second type of realisation, the encrypted data stream can be further encrypted by an exploitation key at the point of transmission, decrypted by an equivalent exploitation key in the security module and then passed in its first encrypted form to
30 the decoder.

As described in all the above embodiments, the data stream passed in encrypted form

-7-

between the security module and decoder may comprise audiovisual data. In such an embodiment, after decryption of the data stream, the decoder will simply display the audio visual data.

5 However, in an alternative embodiment, the data stream passed in encrypted form between the security module and decoder may comprise a control word stream, the decrypted control word stream being used thereafter by the decoder to descramble associated scrambled audiovisual data.

10 In such an embodiment, the " scrambling " and " descrambling " of the control word data stream as described above corresponds to the encryption and decryption of ECM messages using an exploitation key, as in conventional systems.

15 In order to increase the security of the system, any or all of the above described embodiments may implemented in combination with each other.

20 The present invention is particularly applicable to the transmission of a television broadcast. The present invention also extends to a decoder and security module adapted for a method of transmission as described above.

25 The term "portable security module" is used to mean any conventional chip-based portable card type devices possessing, for example, microprocessor and/or memory storage. This may include smart cards, PCMCIA cards, SIM cards etc. Included in this term are chip devices having alternative physical forms, for example key-shaped devices such as are often used in TV decoder systems.

30 The terms " scrambled " and " encrypted " and " control word " and " key " have been used here in a number of ways for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between " scrambled data " and " encrypted data " or between a " control word " and a " key ".

Similarly, whilst the description refers to “ receiver/decoders ” and “ decoders ” it will be understood that the present invention applies equally to embodiments having a receiver integrated with the decoder as to a decoder unit functioning in combination with a physically separate receiver, decoder units incorporating other functionalities, and decoder units integrated with other devices, such as televisions, recording devices etc.

A number of embodiments of the invention will now be described by way of example only and in relation to the attached figures, in which:

10

Figure 1 shows the overall architecture of a known digital television system, as may be adapted by the present invention;

15

Figure 2 shows the conditional access system of the television system of Figure 1;

Figure 3 shows a first embodiment of the invention;

Figure 4 shows a second embodiment of the invention; and

20

Figure 5 shows a third embodiment of the invention.

Digital Television System

An overview of a digital television broadcast and reception system 1000 adaptable to the present invention is shown in Figure 1. The system includes a mostly conventional digital television system 2000, which uses the known MPEG-2 compression system to transmit compressed digital signals. In more detail, the MPEG-2 compressor 2002 in a broadcast centre receives a digital signal stream (typically a stream of video signals). The compressor 2002 is connected to a multiplexer and scrambler 2004 by linkage 2006. The multiplexer 2004 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 2008 of the broadcast centre via linkage 2010, which can of course take

-9-

a wide variety of forms including telecom links. The transmitter 2008 transmits electromagnetic signals via uplink 2012 towards a satellite transponder 2014, where they are electronically processed and broadcast via notional downlink 2016 to earth receiver 2018, conventionally in the form of a dish owned or rented by the end user.

5 The signals received by receiver 2018 are transmitted to an integrated receiver/decoder 2020 owned or rented by the end user and connected to the end user's television 2022. The receiver/decoder 2020 decodes the compressed MPEG-2 signal into a television signal for the television set 2022.

10 A conditional access system 3000 is connected to the multiplexer 2004 and the receiver/decoder 2020, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smart card, capable of decrypting messages relating to commercial offers (that is, on or several television programmes sold by the broadcast
15 supplier), can be inserted into the receiver/decoder 2020. Using the decoder 2020 and smart card, the end user may purchase events in either a subscription mode or a pay-per-view-mode.

An interactive system 4000, also connected to the multiplexer 2004 and the
20 receiver/decoder 2020 and again located partly in the broadcast and partly in the decoder, enables the end user to interact with various applications via a modemmed back channel 4002.

Conditional Access System

25

With reference to Figure 2, the conditional access system 3000 includes a Subscriber Authorization System (SAS) 3002. The SAS 3002 is connected to one or more Subscriber Management Systems (SMS) 3004, one SMS for each broadcast supplier, by a respective TCP-IP link 3006 (although other types of linkage could alternatively
30 be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

-10-

First encrypting units in the form of ciphering units 3008 utilising "mother" smart cards 3010 are connected to the SAS by linkage 3012. Second encrypting units again in the form of ciphering units 3014 utilising mother smart cards 3016 are connected to the multiplexer 2004 by linkage 3018. The receiver/decoder 2020 receives a
5 "daughter" smart card 3020. It is connected directly to the SAS 3002 by Communications Servers 3022 via the modammed back channel 4002. The SAS sends amongst other things subscription rights to the daughter smart card on request.

The smart cards contain the secrets of one or more commercial operators. The
10 "mother" smart card encrypts different kinds of messages and the "daughter" smart cards decrypt the messages, if they have the rights to do so.

The first and second ciphering units 3008 and 3014 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one
15 smart card 3010 and 3016 respectively, for each electronic card, one (card 3016) for encrypting the ECMs and one (card 3010) for encrypting the EMMS.

Multiplexer and Scrambler

20 With reference to Figures 1 and 2, in the broadcast centre, the digital video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 2002. This compressed signal is then transmitted to the multiplexer and scrambler 2004 via the linkage 2006 in order to be multiplexed with other data, such as other compressed data.

25

The scrambler generates a control word CW used in the scrambling process and included in the MPEG-2 stream in the multiplexer 2004. The control word CW is generated internally and enables the end user's integrated receiver/decoder 2020 to descramble the programme. Access criteria, indicating how the programme is
30 commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the

-11-

end user subscribes to one or more commercial offers, of "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels. In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode").

Both the control word CW and the access criteria are used to build an Entitlement Control Message (ECM); this is a message sent in relation with one scrambled program. The message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 3014 via the linkage 3018. In this unit an ECM is generated, encrypted with an exploitation key Cex and transmitted on to the multiplexer and scrambler 2004.

Programme Transmission

The multiplexer 2004 receives electrical signals comprising encrypted EMMs from the SAS 3002, encrypted ECMs from the second encrypting unit 3014 and compressed programmes from the compressor 2002. The multiplexer 2004 scrambles the programmes and transmits the scrambled programmes, the encrypted EMM (if present) and the encrypted ECMs as electric signals to a transmitter 2008 of the broadcast centre via linkage 2010. The transmitter 2008 transmits electromagnetic signals towards the satellite transponder 2014 via uplink 2012.

Programme Reception

The satellite transponder 2014 receives and processes the electromagnetic signals transmitted by the transmitter 2008 and transmits the signals on to the earth receiver 2018, conventionally in the form of a dish owned or rented by the end user, via downlink 2016. The signals received by receiver 2018 are transmitted to the integrated receiver/decoder 2020 owned or rented by the end user and connected to the end

-12-

user's television set 2022. The receiver/decoder 2020 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

5 If the programme is not scrambled the receiver/decoder 2020 decompresses the data and transforms the signal into a video signal for transmission to television set 2022.

If the programme is scrambled, the receiver/decoder 2020 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smart card 3020 of the end user. This slots into a housing in the receiver/decoder 2020. The daughter smart card 3020 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 2020 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 2020 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal onward transmission to television set 2022.

10
15

Subscriber Management System (SMS)

20 A Subscriber Management System (SMS) 3004 includes a database 3024 which manages, amongst others, all of the end user files, commercial offers (such as tariffs and promotions), subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS

25 Each SMS 3004 transmits messages to the SAS 3002 via respective linkage 3006 to enable modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

The SMS 3004 also transmits messages to the SAS 3002 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

30

Entitlement Management Messages and Entitlement Control Messages

ECMs or Entitlement Control Messages are encrypted messages embedded in the data stream of a transmitted program and which contain the control word necessary for descrambling of a program. Authorisation of a given receiver/decoder is controlled by EMMs or Entitlement Management Messages, transmitted on a less frequent basis and which supply an authorised receiver/decoder with the exploitation key necessary to decode the ECM.

10 An EMM is a message dedicated to an individual end user (subscriber), or a group of end users. A group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.

15 Various specific types of EMM may be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services. So-called " Group " subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap

20

For security reasons, the control word CW embedded in an encrypted ECM changes on average every 10 seconds or so. In contrast, the exploitation key Cex used by the receiver to decode the ECM is changed every month or so by means of an EMM. The exploitation key Cex is encrypted using a personalised key corresponding to the identity of the subscriber or group of subscribers recorded on the smart card. If the subscriber is one of those chosen to receive an updated exploitation key Cex, the card will decrypt the message using its personalised key to obtain that month's exploitation key Cex.

25
30 The operation of EMMs and ECMs will be well-known to one skilled in the art and will not be described here in any more detail.

Encryption of Data Stream by Smart Card

Referring now to Figures 3 and 4, a number of embodiments of a first realisation of the present invention will now be described. As shown in Figure 3, a scrambled
5 audiovisual data stream is received by the receiver/decoder 3020 and passed to the portable security module 3020 where it is descrambled at 3030 using the exploitation key Cex possessed by the card to generate the decrypted control word CW and thereafter descramble the transmission. As will be understood, in this invention, the descrambling of a transmission is carried out entirely on the portable security module,
10 which may comprise a smart card, a PCMCIA card etc.

Before being passed back to the decoder, the data stream is re-encrypted according to a first encryption key Kf at 3031. The operation of the key Kf is dependant on a decoder identity value N associated with the identity of the decoder, for example its
15 serial number. This value N is communicated to the card by means of an encrypted EMM, transmitted at the initialisation of the decoder/card system and passed by the decoder 2020 to the card 3020 for decryption at the point 3032.

As with all EMM messages, the EMM containing the identity value N is encrypted
20 by means of a personalisation key corresponding to a key held by the card and known by the transmitter of the message, which enables that card or group of cards to decode the encrypted EMM.

In an alternative embodiment, the initialising EMM can be pre-stocked in the memory
25 of the decoder and sent to the card upon the first insertion of the card, or each time the decoder is turned on. In the latter case the card will be programmed to accept the initialising EMM only the first time that it receives it. Again, as with the transmitted EMM, the personalisation key associated with the card will be used to encrypt and decrypt the transmitted value.

30

Turning now to the decoder 2020, this is also provided with a key Kf and, of course, its identity or serial number N. The key Kf and number N may be stocked, for

-15-

example, in the ROM of the decoder. Using the key Kf and identity value N, the decoder decrypts the descrambled data stream. In practice the identity value need not be fixed, and it would be a simple matter to reprogram the identity value N stored within the card and decoder if this proved necessary.

5

In this embodiment, the key Kf can most simply be created using any known symmetric key algorithm for generating a key capable of being diversified by a given value (such as the identity value N in the above example). A public/private key pairing is also conceivable, the public key being associated with the decoder, the private key with the smart card. As in conventional systems, the exploitation key and personalisation key may be generated by a symmetric algorithm.

10

As will be understood, the data stream is only transmitted between the card and decoder in an encrypted or scrambled form, thereby reducing the risk of the type of fraud described in the introduction of the application. Furthermore, in this embodiment, all communications between the card and decoder are in fact encrypted, thereby increasing the security of the system.

15

In the above embodiment, the data stream decrypted at 3030 and re-encrypted at 3031 corresponds to a stream of audiovisual data. In an alternative embodiment, the data stream may correspond to a stream of control word data, decryption of ECMs being carried out at 3030 to generate a control word stream re-encrypted at 3031 and communicated to the decoder. The decrypted control word stream produced at 3033 by the decoder is thereafter used by the decoder to descramble scrambled audiovisual data transmitted and associated with the control word stream.

20

25

The advantage of such an embodiment is that the circuitry necessary to process and descramble the flow of audiovisual data is embodied within the decoder, rather than in the security module, which handles only the decryption and re-encryption of the control word stream.

30

One drawback of the system of Figure 3 lies in the fact that, although not trivial, the

-16-

extraction of the key K_f and identity value N from the ROM of the decoder may be carried out without too much difficulty. The embodiment of Figure 4 overcomes this weakness.

- 5 As shown, a random or pseudo-random number RN is generated within the decoder at 3040 and passed for subsequent encryption at 3041 by a public key K_{pub} of a suitable public/private key algorithm, such as RSA. The corresponding private key K_{pri} is held by the smart card. The encrypted random number $p(RN)$ is then passed to the smart card which uses the private key K_{pri} to decrypt at 3042 the encrypted
10 random number value $p(RN)$.

- As with the identity value N in the previous embodiment, the value RN is used at 3031 in the encryption by a symmetric key K_f of the descrambled data stream so as to obtain an encrypted data stream then passed from the card to the decoder. The
15 communication of the original scrambled data stream from the decoder to the smart card has been omitted here in order to simplify the diagram.

- On the side of the decoder, the encrypted value data stream is decrypted at 3033 using the symmetric key K_f and the random number value RN . Unlike the identity value
20 N of the previous embodiment, the random number RN can be a frequently changing value stored in the RAM of the decoder and, as such, relatively difficult to identify. The public key K_{pub} and symmetric key values are stored in a more permanent fashion in the device and, as such, are less secure. However, even in the event that an unauthorised user manages to obtain these keys, and the encrypted value $p(RN)$,
25 it will not be possible to generate the RN value needed to decrypt the data stream from this information because of the nature of private/public key algorithms and the security of the control word will remain uncompromised.

- The same public/private key pair can be used for a series of decoders and cards.
30 However, the level of security will be increased through the use of a unique public/private key pair associated with that smart card.

-17-

As shown, the values of Kpub and Kpri are generated by the system operator shown at 3050 and embedded in the smart card 3020. The value of Kpub will then be communicated to the decoder at the moment of insertion of the smart card in the decoder. Since the public key Kpub will be used to encrypt the random number RN it is used important for the decoder to verify the origin of this key, for example to prevent the decoder communicating information in response to the reception of a public key belonging to a fraudulent user.

To this end, the public key Kpub is encrypted by a private key KeyG unique to the operator and shown at 3051, the certificate containing Kpub thereafter being communicated to and stored in the smart card 3020 at 3052. At the moment of insertion of the card in the decoder, the certificate is decrypted and authenticated by the decoder at 3053 using the equivalent public key KeyG stored at 3054. The value of Kpub thus obtained will thereafter be used for the subsequent encryption steps.

Whilst the data stream described at 3030 and re-encrypted at 3031 has been described in relation to audiovisual data, this may equally correspond to a stream of control word data. As before, in such an embodiment, ECMs containing the control word are decrypted at 3030 and re-encrypted at 3031 for transmission to the decoder. The decrypted control word data obtained at 3033 is then used by the decoder to descramble an associated audiovisual data stream.

Encryption of Data Stream at Transmitter

The above embodiments relate to a first type of realisation of the invention in which the encryption of the data stream communicated from the card to the decoder is carried out by the smart card itself. In the following embodiment, an alternative realisation will be described with reference to Figure 5 in which the encryption is carried out further upstream, at the transmitter. As will become clear, this is in addition to the conventional encryption or scrambling of the data stream.

Figure 5 represents the flow of information in this embodiment between the

transmitter 2008, smart card 3020 and decoder 2020. As will be appreciated, whilst this figure shows the information being transmitted directly between transmitter and smart card in order to simplify the explanation, any signals received by the smart card will have of course been received and communicated to the card via the receiver/decoder unit. Similarly, whilst the transmitter has been represented as a single functional block in this case, the encryption of the transmitted message may be carried out by separate elements of the system, as described in relation to Figures 1 and 2.

10 In this embodiment, the audiovisual data stream is encrypted at 3050 by an encryption key K_t , the exact value of which is dependant on a universal variable t known to all elements of the system, for example, the real time and/or date of transmission. The encrypted data $f(\text{DATA})$ is then scrambled as in conventional systems at 3051 by a control word and the resulting encrypted and scrambled data transmitted and communicated to the security module 3020 within the decoder 2020. The scrambled data is then descrambled at 3020 by the security module.

Unlike existing systems, the data will still be in an encrypted form $f(\text{DATA})$ and will be passed in this form to the decoder 2020 for decryption at the point 3052. The decoder 2020 also possesses an equivalent of the key K_t and, if universally available information such as time and/or date is used, will also be in possession of the value t . The data may then be decrypted and processed by decoder.

By using a changing universal variant, the system avoids the problem that any recording of the encrypted control stream $f(\text{CW})$ obtained by monitoring the card/decoder communications could be used by unauthorised users in the future, since the control stream usable at the moment of transmission will not be usable by a decoder at a future time/date. In contrast, the fact that a universal variable is chosen means that no explicit communication of this variable between the transmitter/decoder is necessary.

In the above described embodiment, the security module 3020 carries out on-board

-19-

descrambling of the encrypted and scrambled data, using an exploitation key to decrypt a stream of ECM data (not shown) so as to obtain control word data needed for the first descrambling step.

- 5 In an alternative embodiment, the steps shown in Figure 5 may be carried out on the control word data itself, by encrypting at 3051 the once-encrypted control word data using an exploitation key C_{ex} , carrying out a first decryption on the card 3020 using the equivalent exploitation key and thereafter carrying out a second decryption at 3052 using the value t to obtain control word data in clear form. This may then be used
- 10 to descramble associated scrambled audiovisual data received by the decoder.

Whilst less secure than the previous embodiments, this type of system has the advantage that it may be simply implemented in existing systems without any need, for example, to generate new smart cards and the modifications needed to the decoder

15 and transmitter units may be introduced by reprogramming.

As will be understood, all of the embodiments described with reference to Figures 3 to 5 may be implemented separately or in any combination to increase the level of security, if required.

CLAIMS

1. A method of transmission and reception of a scrambled data stream in which the
5 scrambled data stream is transmitted to a decoder and thereafter passed to and
descrambled by a portable security module inserted in the decoder and characterised
in that the data stream is passed from the security module to the decoder in an
encrypted form, to be decrypted and subsequently used by the decoder.
- 10 2. A method as claimed in claim 1, in which the data stream is encrypted in the
security module by a first encryption key before being passed back to the decoder for
decryption using an equivalent of the first key.
- 15 3. A method as claimed in claim 2 in which the data stream is encrypted in the
security module by a first encryption key variable in dependence on a decoder identity
value, the decoder possessing an equivalent of the key and value necessary to decrypt
the data stream.
- 20 4. A method as claimed in claim 3 in which the decoder identity value is encrypted
by a personalised key known to the security module and transmitter, the decoder
identity value being transmitted in an encrypted form to the decoder for
communication to the security module.
- 25 5. A method as claimed in 3 in which the decoder identity value is encrypted by a
personalised key known to the security module, the encrypted decoder identity value
being stored in the decoder during manufacture for communication to the security
module upon insertion of the security module in the decoder.
- 30 6. A method as claimed in claim 2 in which the data stream is encrypted in the
security module by a first encryption key dependant on a random or pseudo-random
number.

7. A method as claimed in claim 6, in which the random number is communicated between the decoder and security module encrypted by a second encryption key.

5 8. A method as claimed in claim 7, in which the random number is generated and encrypted by the second encryption key in the security module and communicated to the decoder for decryption by an equivalent of the second key stored in the decoder.

10 9. A method as claimed in claim 7 in which the random number is generated and encrypted by the second encryption key at the decoder and communicated to the security module for decryption by an equivalent of the second key stored in the security module.

15 10. A method as claimed in claim 9 in which the second key used to encrypt the random number in the decoder corresponds to a public key, the security module being provided with the equivalent private key necessary to decrypt the random number value.

20 11. A method as claimed in claim 9 or 10 in which at least the second key held by the security module is unique to that security module.

25 12. A method as claimed in any of claims 7 to 11, in which the second key held by the decoder is encrypted by a third key before communication to the decoder, the decoder possessing the corresponding third key so as to hereby decrypt and verify the second decoder key.

13. A method as claimed in claim 12, in which the third key used to encrypt the second decoder key is a private key, the decoder possessing the equivalent public key to decrypt and verify the communicated second key.

30 14. A method as claimed in claim 1 in which the data stream is encrypted at the point of transmission by a first encryption key and decrypted by the decoder by an equivalent of this key.

15. A method as claimed in claim 14 in which the data stream is encrypted at the point of transmission by a first encryption key dependant on a variable known to both the transmitter and the decoder and decrypted at the decoder by an equivalent of this key and variable.

5

16. A method as claimed in claim 15 in which the variable corresponds to the real time and/or date of transmission.

10

17. A method as claimed in any of claims 14 to 16 in which the first encrypted data stream is further scrambled at the point of transmission, descrambled in the security module and then passed in its first encrypted form to the decoder.

15

18. A method of transmission and reception of scrambled data combining a method of encryption of the data stream in the card as claimed in any of claims 2 to 13, separately or in combination, together with a method of encryption of the control word at the point of transmission, as claimed in any of claims 14 to 17.

20

19. A method as claimed in any of claims 1 to 18 in which the data stream passed in encrypted form between the security module and decoder comprises audiovisual data.

25

20. A method as claimed in any of claims 1 to 18 in which the data stream passed in encrypted form between the security module and decoder comprises a control word stream, the control word stream once decrypted by the decoder being thereafter used by the decoder to descramble associated scrambled audiovisual data.

30

21. A method as claimed in any preceding claim in which the scrambled data stream is transmitted as part of a television broadcast.

22. A decoder and portable security module adapted for use in a method as claimed in any preceding claim.

-23-

23. A method of transmission and reception of a scrambled data stream substantially as herein described.

Fig.1.

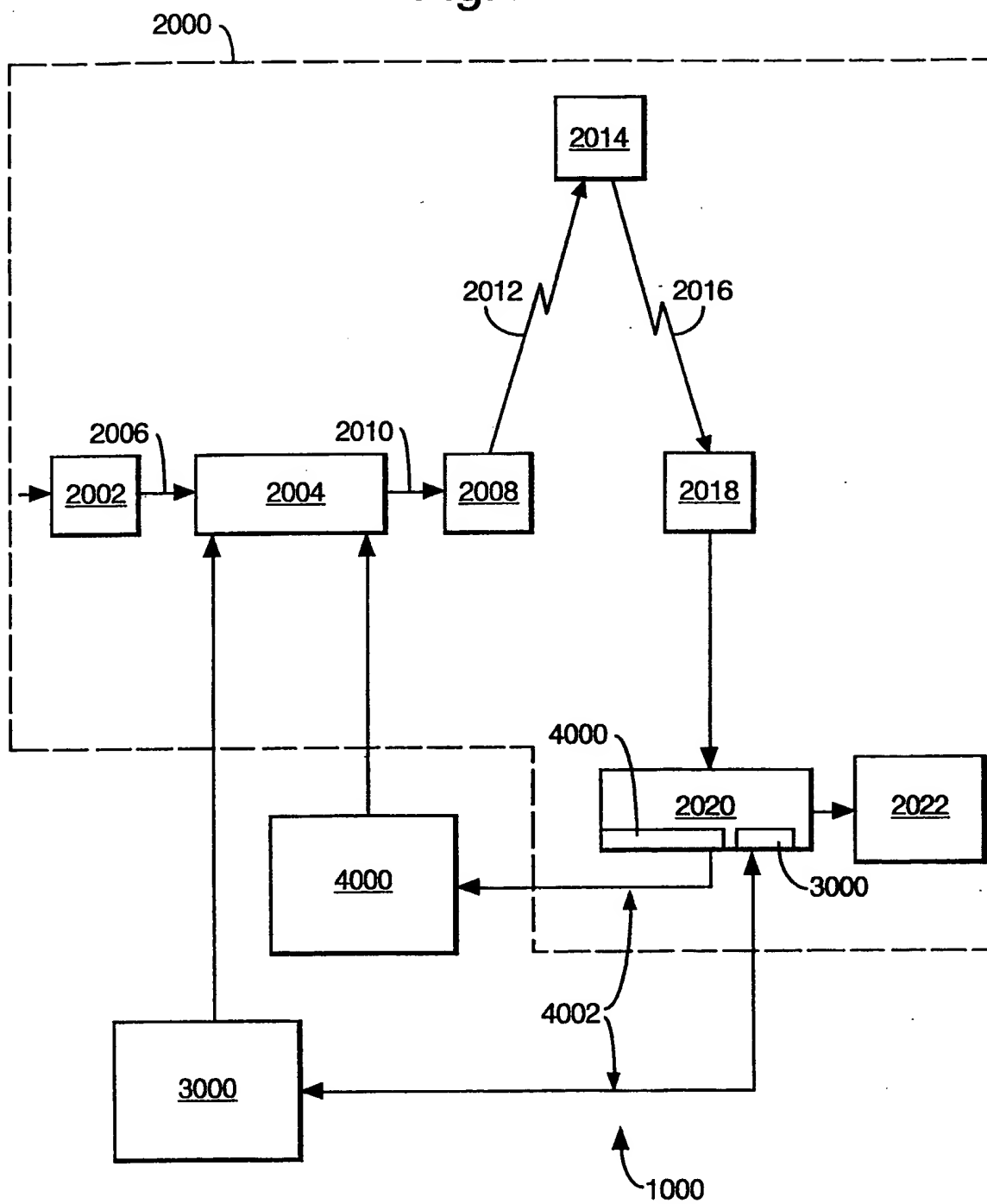


Fig.2.

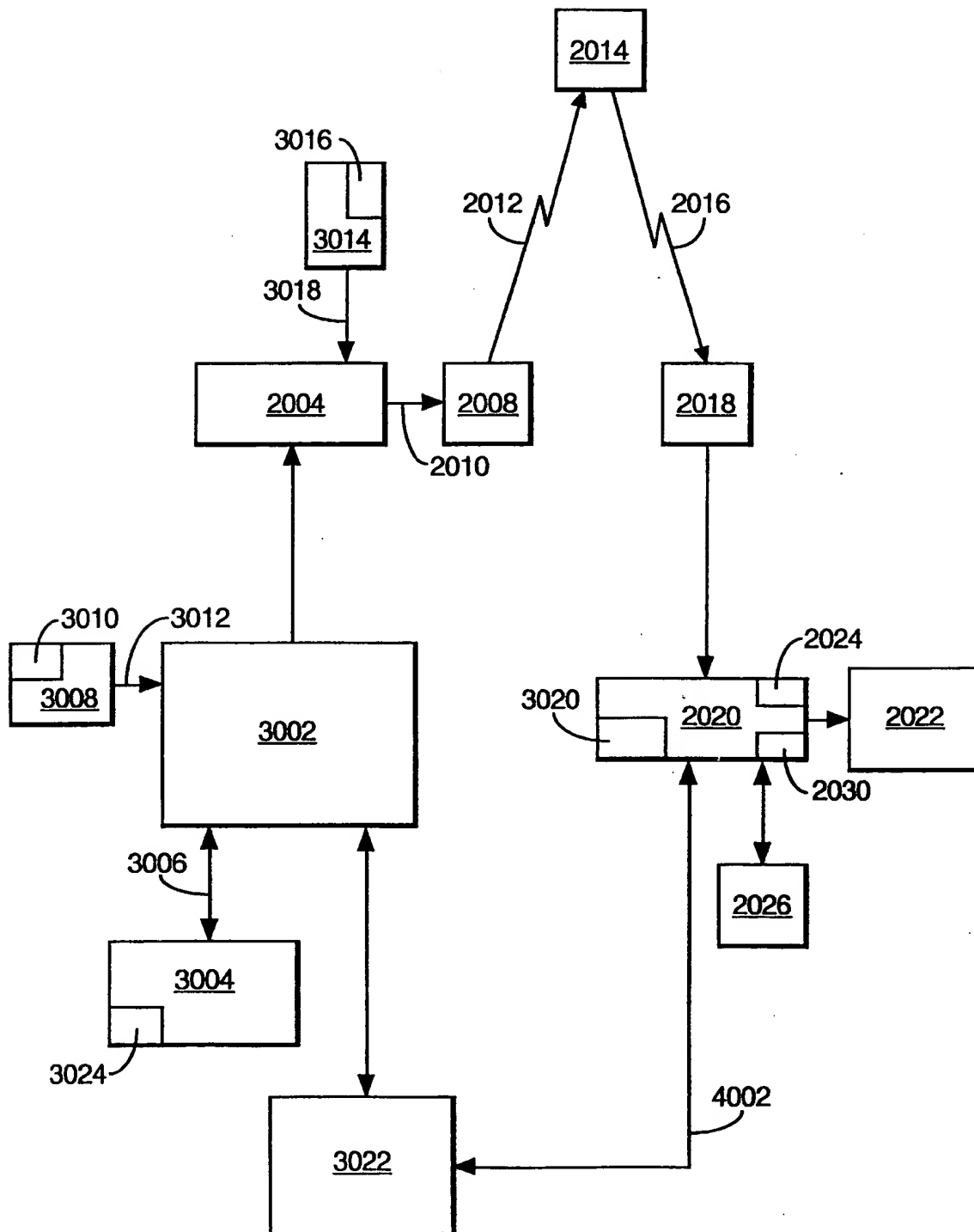


Fig.3.

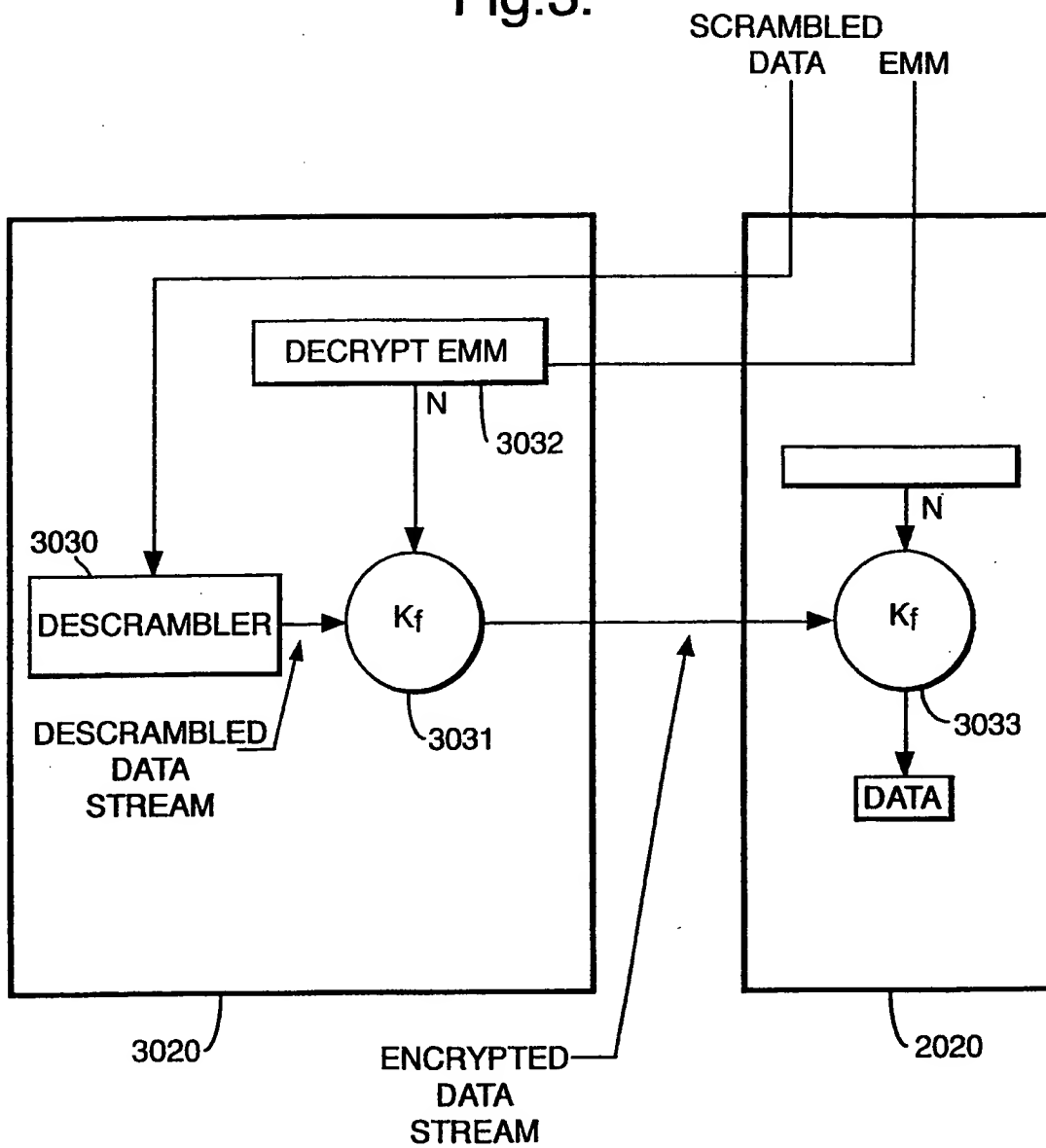


Fig.4

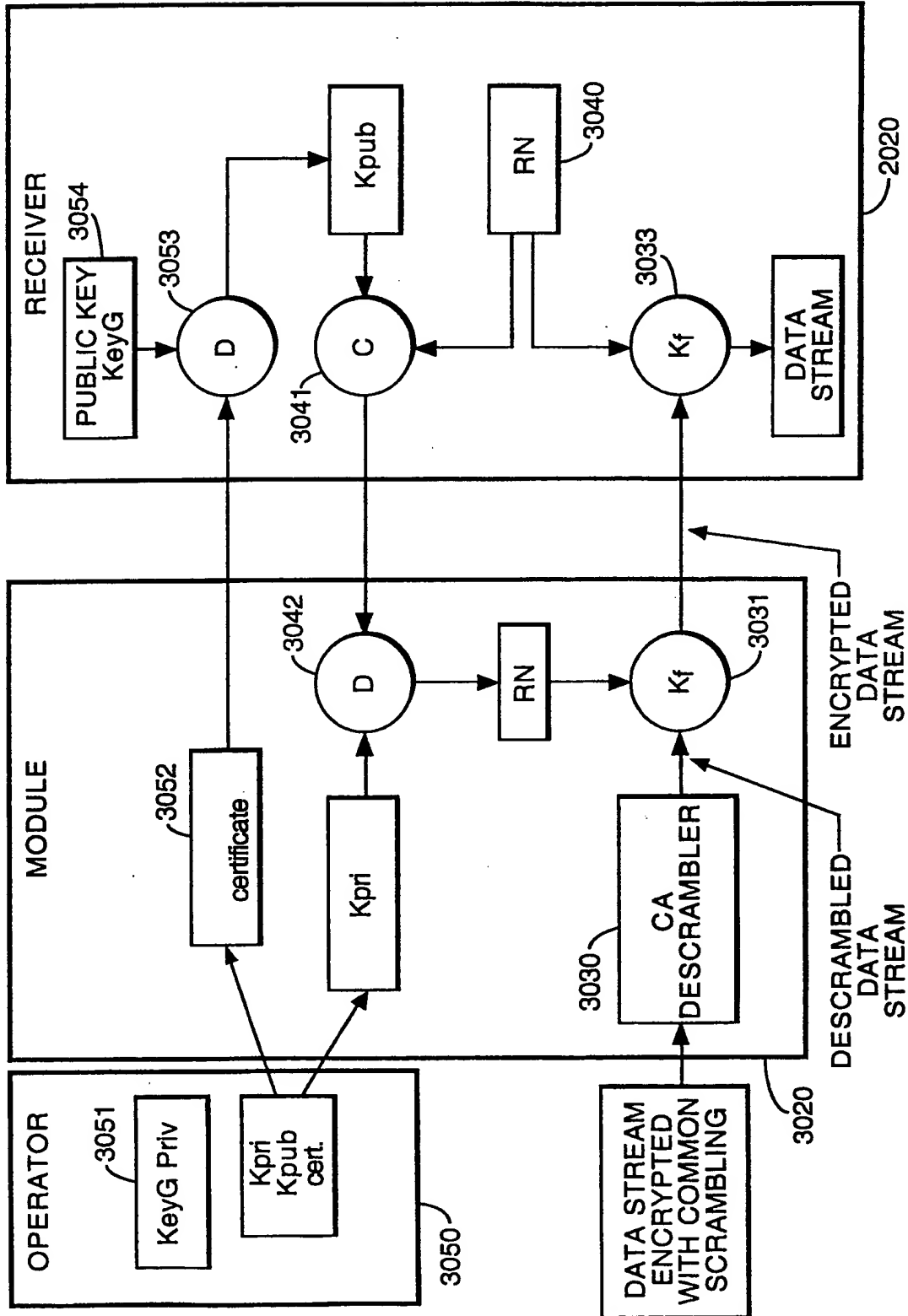
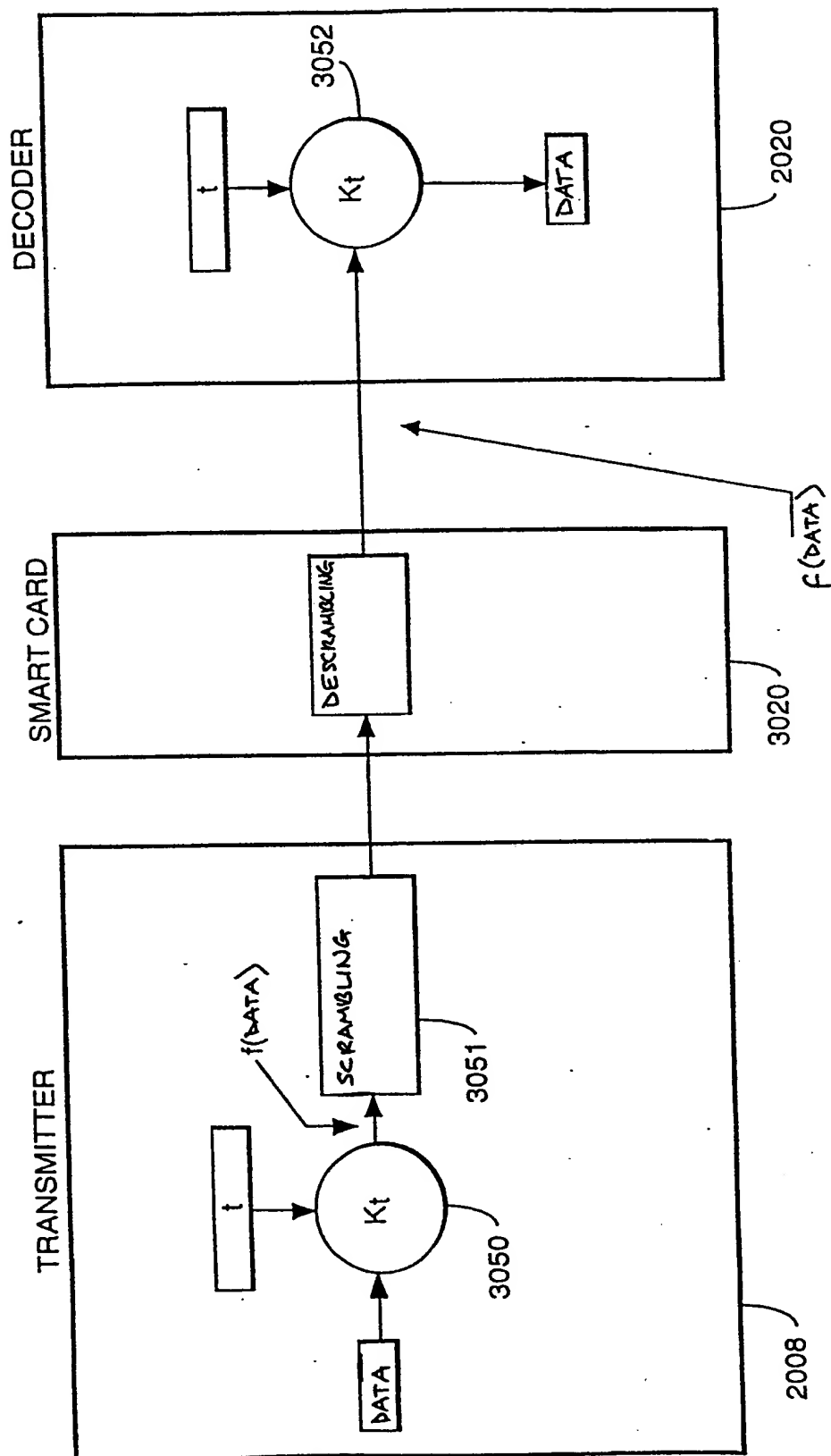


Fig.5.



INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 98/01610

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 06504 A (THOMSON CONSUMER ELECTRONICS ;CHANEY JOHN WILLIAM (US)) 29 February 1996 see page 3, line 25 - page 4, line 13 see page 15, line 17 - page 17, line 6 see figures 1,4	1,2, 14-18, 20,23
A	EP 0 599 366 A (SCHLUMBERGER IND SA) 1 June 1994 see page 2, column 2, line 19 - page 3, column 3, line 19 see figure 1	1,2,20, 23

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

23 November 1998

Date of mailing of the international search report

04/12/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Verleye, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 98/01610

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
EP 0599366 A	01-06-1994	FR 2698510 A	27-05-1994
		AT 166761 T	15-06-1998
		DE 69318805 D	02-07-1998
		JP 6350594 A	22-12-1994
		US 5509073 A	16-04-1996